Application No.: 09/767,902 Docket No.: 00-VE04.75A CIP

REMARKS

Claims 1, 26 and 30 are amended to include language emphasizing advantageous features of the invention previously brought to the attention of the Examiner that further distinguish the subject matter sought to be protected over the applied art. Claims 3, 6, 7, 8, 18, 28 and 32 are also amended to more clearly define the subject matter considered to be the invention as disclosed. While it is believed that the language of the claims as previously presented describe subject matter distinguishable and thereby patentable over the applied art, to advance prosecution of the application and allowance of patentable subject matter describe subject matter, independent claims 1 and 26 are amended without disclaimer or prejudice to include claims of similar, broader, or any other scope supported by the disclosure in a continuing application. Specifically, to further emphasize that an embodiment of the invention is directed at protecting a communications network from harmful control messages arising either inside or outside the network, independent claim 1 is amended to require that the signaling system security monitor include:

> "a plurality of message templates corresponding to approved individual ones of said control data messages, sequences of such control data messages and informational relationships between the data contents of such data messages, said system security monitor being responsive to said message templates to perform syntax and content dependent screening of said control data messages, said content dependent screening including checking appropriateness of said control data messages in context of (i) a state of the communications network and (ii) prior related messages."

The revised language emphasizes important aspects of certain embodiments of the invention including features of the template. That is, according to an aspect of the invention, a template for a transaction is much more than a series of individual templates for the messages of that transaction. As captured by the amended language, a template contains the information about the relationships between messages of a call or transaction and their respective parameters and parameter values. The applied art fails to teach or suggest this and other features of the invention as now recited by the amended claims.

Support for the added language can be found in the Specification as filed including:

Page 9, lines 23 – 25:

...It [message checking] may also be enhanced by defining required relationships between successive messages associated with a call or transaction.

Page 10, lines 4 – 15:

A Security Gatekeeper (alternatively referred to as a Signaling System Security Monitor) according to the invention, screens down to the application layer and inspects for inappropriate application messages, parameters and/or parameter values as well as inappropriate relationships between messages. In the case of certain violations, the Gatekeeper modifies messages (e.g., removes a parameter, modifies a parameter value, etc.), rather than merely allowing the message to progress into and/or through the network or rejecting and discarding non-conforming messages. This is accomplished, in part, by screening in context, maintaining the state of ongoing signaling exchanges (e.g., call setup, application query/response) and rejecting or modifying messages that are inappropriate to the current state of the exchange and, as necessary, generating corrective messages. This context screening maintains network operations and avoids "hanging up" the network in an unstable state.

Page 10, line 26 - page 11, line 5:

The Security Gatekeeper further facilitates screening based on a protocol definition of an allowable exchange, i.e., using sets of templates. The Security Gatekeeper permits the network operator to provision the gateway to permit message exchanges that are consistent with a predetermined agreed to service definition (while discarding or modifying messages inconsistent with that definition). These template definitions can include allowable messages, message sequences, message parameters, and parameter values and can also specify the relationship between parameters in successive messages (e.g., same phone number in query and response). For example, the Security Gatekeeper may use a template check to prohibit an AIN message from inappropriately modifying billing records, such as charging a call to someone else's account.

Page 11, line 6 – 14:

State-based screening examines messages based on the context in which the messages arrive. To implement state-based screening, the Security Gatekeeper maintains information on the states of calls and/or transactions for which the screening is performed. Examples include Call Setup and Transaction query/response. The Security Gatekeeper maintains the status of the underlying state machines, which define the possible call and/or transaction states and the legitimate transitions from one state to another as well as the relationships between parameters in successive messages. Such a state transition table or graph would be used, for example, to allow an ACM, ANM or REL message in response to an IAM, but would prohibit an RLC message.

Page 11, line 28 - page 12, line 2:

For responses or other successive messages, the templates identify message types, mandatory and optional parameters and value ranges, and, in addition, the relationship between parameters and parameter values in the initial message and those in successive messages. For example, if a query identifies a specific telephone number, the response can likewise be required to pertain to that specified telephone number.

Page 12, lines 14 – 23:

Thus, the template methodology implemented by the Security Gatekeeper forms a common ground for agreement, defining the signaling that will be exchanged, without necessarily disclosing or defining the service that will be provided or the details of its implementation. The template definitions can also be used to help certify the proposed application. Once an application has been certified, the Security Gatekeeper monitors transactions on an ongoing basis to ensure that each conforms to the appropriate template. By enforcing the agreed to protocol definition of the application, the Security Gatekeeper insulates the network operator from concerns about the safety and stability of the application while providing the third party service provider the flexibility to make non-protocol affecting changes to the service and to protect its intellectual property.

Page 14, lines 3 – 9:

According to a feature of the invention, the signaling system security monitor is configured to selectively pass the control data messages between the signaling gateway and the signaling communication system if they pass the contextual tests implicitly specified in the appropriate templates. The signaling system security monitor may further be configured to selectively enable and inhibit the signaling gateway from exchanging the control data messages between the remote communication network and the signaling communication system.

Page 24 (see table):

Category	Description
Context-dependent	Appropriateness of message in view of prior related messages and expected/allowed message sequencing, existing service agreements, state of the network, privilege levels associated with

Screening	OPC, DPC, CdPA and CgPA, etc.

Page 26, lines 27 – 30:

> These additional functions include context based checks ensuring that message content and the network=s reaction to the message are appropriate in view of the state of the network including previously generated messages.

Similar language has been added to independent claim 26 and claim 30 dependent therefrom to render those claims together with claim 1 patentably distinguishable over the applied art. Contrary to the Examiner's position the recited functionality differs from that which may or may not be performed by a switch - i.e., maintain state of calls and transactions, or parse messages for allowed syntax. As distinguished from an individual switch, there are two major security advantages of performing screening at the periphery of a network.

One difference between a switch and the functionality provided by a signaling system security monitor is that, in the case of the latter, screening that is performed at the periphery of the network can be sensitive to the route by which the traffic entered the network (e.g., did it come over linkset 1 from network 1, or over linkset 2 from network 2?). Once traffic has been routed to a destination (such as a switch), the destination can no longer ascertain that the message was handed off by network 1 or network 2. It can determine whether the sending address is appropriate, but it can't determine whether it came from a network that should be delivering traffic from that sending address. For example, an analogous situation may be if you receive a call from a colleague who tells you to meet them in front of your office in 5 minutes, you'll go down and meet them. If you knew that the call came from a number in Idaho, you'd be suspicious, even though everything else about the call seems legitimate.

Another advantage provided by a centralized, periphery-based screening function is that it allows screening to be updated by one party, and in one place. If a threat is identified, there is no need to alter the operation of each and every switch in the network to protect against the threat. Instead, the threat can be addressed by upgrading protection at the centralized screening point, i.e., at the signaling gateway and/or the system security monitor.

Further, the operator of the device can establish the desired level of protection, rather than relying on whatever has been implemented by switch manufacturers.

As detailed, these are significant reasons and advantages to screening control messages at the periphery of the network and not the end node.

As described, screening includes several steps. First, control data messages are screened for appropriate syntax. Syntax screening tells whether a message can be correctly and unambiguously decoded per the standard set of message definitions. Thus, according to an embodiment of the invention, every parameter is checked to make sure that it is a legitimate parameter for that message, and every parameter value is checked, to make sure that it is defined and meaningful for that parameter.

Second, content is screened. Content deals with the values contained in syntactically correct messages

Third, the control data message is screened for context. Context examines a message with respect to related messages sent (or not sent) before. Embodiments of the invention include two kinds of context screening. The first is with respect to a state machine. Given the state of a trunk or a transaction, certain messages are appropriate and others are not. For example, a call cannot be answered if no call has not been previously placed; a response to a query is improper if no query has been previously sent.

The second type of context screening combines aspects of both content and context screening. This type of screening allows for the definition of services as acceptable exchanges of messages in compliance with specific sets of rules. Those rules have aspects of both content and context, referred to in the disclosure as templates. For purposes of the present explanation, these may be considered as message templates and service templates. Message templates define the specific allowable structures of otherwise generalized message, e.g., AIN messages that will be associated with a service. As with the templates that might be used for content screening, these templates define the required, permissible and prohibited parameters that may be included in the message, the permissible values of those parameters, and any interrelationships between the parameters of a single message. Service templates are similar to state machines in that they define the set of messages that would be acceptable

given the current state of an exchange. They go a step further, however, in identifying any relationship tests that must be met by the related messages - for example, it might require that the outgoing telephone number specified in one message correspond to the incoming telephone number specified in a prior message.

One of the advantages of context screening as disclosed and explained in Applicants' disclosure is that it allows a party whose equipment is being controlled by another party to monitor whether the controlling party is living up to the agreements that were made as to the nature of the control that is being exerted. The prior art fails to suggest, much less describe or enable, this type of protection of a network including:

> *a signaling system security monitor, separate from the central office switching systems, said signaling system security monitor including a plurality of message templates corresponding to approved individual ones of said control data messages, sequences of such control data messages and informational relationships between the data contents of such data messages, said signaling system security monitor being responsive to said message templates to perform syntax and content dependent screening of said control data messages, said content dependent screening including checking appropriateness of said control data messages in context of (i) a state of the communications network and (ii) prior related messages.*

For the reasons present, independent claims 1 and 26 (the latter alone and in combination with dependent claim 30) are considered to be patentably distinguishable and allowable over the applied art.

Each of the dependent claims is also believed to be distinguishable and patentable over the art of record both as dependent from the allowable subject matter of their respective base and any intervening claims and by including further subject matter not found in or suggested by the art of record. For example, claim 9 recites:

> *The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing states of respective ones of said central office switching systems, said signaling system security monitor responsive to said states for selecting ones of said templates.*

As fully detailed above, the prior art fails to describe or suggest a signaling system security monitor storing and responding to the state of a plurality of separate central office switching systems.

The outstanding rejections of the claims are further believed to be improper for lack of motivation for combining the references as applied by the Examiner.

> The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985).

M.P.E.P. §706.02(j): Contents of a 35 U.S.C. 103 Rejection and §2143.01: Suggestion or Motivation To Modify the References - The Prior Art Must Suggest The Desirability Of The Claimed Invention.

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

Id.

The Examiner's reasoning for combining the references is that:

> *...it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the feature of having a signaling gateway that is configured to exchange said control data messages between two communication networks, as taught by Heilmann, into the Silva system in order to ensure that the messages, that are received and sent to each network already screened, verified, and filtered based on the set rules.*

Office Action at page 4.

However, the Examiner's rationale is flawed since there is no recognition by the applied art of the problems nor any suggestion for making the asserted combination so as to address such a problem.

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." (916 F.2d at 682, 16 U.S.P.Q.2d at 1432.).

It is well established that, even if all aspects of the claimed invention were individually known in the art, such is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). It is, therefore, incumbent upon the Examiner to provide some suggestion of the desirability of doing what the inventor has done in the Examiner's formulation, imposition and maintenance of a rejection under 35 U.S.C. 103(a). "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 U.S.P.Q. 972, 973 (Bd. Pat. App. & Inter. 1985).

Thus, for the reasons presented, the rejection of all claims is believed to be improper and withdrawal thereof is respectfully requested.

In summary, claims 1 – 32 are now considered to be in condition for allowance. Favorable reconsideration of the application, as amended, and an early notification of allowance are respectfully requested.

Applicants have filed concurrently herewith a Petition for a Three-Month Extension of Time. However, if any other or additional fee is due, please charge our Deposit Account No. 07-2347 from which the undersigned is authorized to draw and please credit any excess fees to such deposit account.

Application No.: 09/767,902

Docket No.: 00-VE04.75A CIP

Respectfully submitted,

Joseph R. Palmieri Reg. No 40,760

Verizon Corporate Services Group
600 Hidden Ridge Drive
Mail Code: HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127

Date: March 2, 2006

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being transmitted by facsimile to the United States Patent Office at 571-273-8300.

Dated: March 2, 2006 Signature: (Christian R. Andersen)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.